Personal data protection in the criminal process: experience of the European Union and realization in Ukraine

Захист персональних даних у кримінальному провадженні: досвід Європейського Союзу та реалізація в Україні

Yaroslav Bereskyi, Valentyn Muradov

Key words:

data protection, safety of data transfer, safety of investigation parties, safety of data storage.

Ключові слова:

захист персональних даних, безпека передачі даних, безпека учасників провадження, безпечне зберігання персональних даних.

Як відомо, під час кримінального провадження акумулюється величезний обсяг персональних даних його учасників. Зважаючи на сучасний рівень розвитку інформаційно-комунікаційних технологій і специфічний характер діяльності органів кримінальної юстиції в рамках провадження, увесь масив персональних даних окремих осіб фактично концентруються в матеріалах окремого об'ємного документа – кримінального провадження. Це можуть бути загальні персональні дані (ідентифікаційні дані (прізвище, ім'я, по батькові, адреса, телефон тощо), паспортні дані, особисті відомості (вік, стать, сімейний стан тощо), склад сім'ї, освіта, професія, біометричні дані (зріст, вага, дактилоскопічні дані, особливі прикмети тощо), психологічні дані (особистісні дані, характер, темперамент тощо), житлові умови, спосіб життя, життєві інтереси та захоплення, споживчі звички, фінансова інформація, електронні ідентифікаційні дані (трафік, IP-адреса тощо), електронні дані про локалізацію (GSM, GPS тощо), запис зображень (фото, відео), звукозапис. Також такими даними можуть бути й особливі персональні дані, такі як расова приналежність, політичні погляди, релігійні та світоглядні переконання, членство в політичних партіях і професійних спілках, стан здоров'я, стан статевого життя.

Політика країн ЄС спрямована на створення передумов щодо реального захисту таких даних, а саме: здійснення контролю над відповідністю процесу обробки персональних даних, що виконується як на рівні наддержавних органів ЄС, так і державних (муніципальних) установ, приватних структур, вимогам законодавства ЄС. З появою у 1960-х роках інформаційних технологій з'явилася потреба в розробленні більш досконалих (детальних) правил забезпечення захисту осіб через охорону їхніх (персональних) даних. До середини 1970-х років Комітет міністрів Ради Європи прийняв ряд резолюцій про захист персональних даних із посиланням на статтю 8 ЄКПЛ. У 1981 році була відкрита для підписання Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (далі – Конвенція 108). Конвенція 108 була й залишається єдиним юридично зобов'язуючим міжнародним документом у сфері захисту персональних даних. Після набуття чинності Лісабонським договором у грудні 2009 року Хартія основних прав ЄС стала юридично обов'язковим документом, а разом із цим статусу окремого основоположного права набуло право на захист персональних даних. Усі держави-члени ЄС ратифікували Конвенцію 108. У 1999 році до Конвенції 108 було внесено зміни, які дозволили ЄС стати стороною Конвенції. У 2001 році було прийнято Додатковий протокол до Конвенції 108, який містить положення про транскордонні потоки даних до так званих третіх країн, які не є сторонами, та про обов'язкове створення національних наглядових органів із питань захисту персональних даних.[1]

У свою чергу Україна ратифікувала Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних і Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних (Закон України

[1] Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2015. С. 16–18.

від 6 липня 2010 р. №2438-VI*)*. Також були прийняті закони та підзаконні нормативно-правові акти, спрямовані на закладення основ такої діяльності[2].

Хоча варто додати, що сьогодні функції Державної служби України з питань захисту персональних даних (колишній центральний орган виконавчої влади з питань захисту персональних даних) перебрав на себе Департамент із питань захисту персональних даних Секретаріату Уповноваженого Верхової Ради України з прав людини.

Загалом же чинне законодавство України містить близько 3500 нормативно-правових актів, які регламентують правові відносини, пов'язані з обігом інформації про фізичну особу (персональні дані). Більшість із них конкретизує зміст інформації про особу виключно щодо сфери правового регулювання трудових, адміністративних або кримінально-процесуальних правовідносин. Зміст цієї інформації має розрізнений характер і не підпорядковується єдиним критеріям[3].

З точки зору наукових досліджень цієї проблематики можна виділити ряд учених, котрі працювали над цим питанням, а саме: А. Анісімова, І. Арістову, О. Баранова, Ю. Батурина, І. Бачила, З. Богатиренко, І. Бочкарьову, В. Брижка[4], Д. Василенка[5], Н. Грицяк, А. Гуз[6], В. Дзюндзюка, П. Діхтієвського[7], А. Марущака, О. Жуковську, Є. Захарову, В. Іванського, І. Кісельова, М. Лапчинського, В. Ліпкана, А. Левенчука, А. Лушнікова, М. Лушнікову, І. Маміофа, Р. Марутян, А. Минькова, Є. Муньє, Т. Обуховську[8], О. Оніщенка[9], А. Пазюка[10], М. Різака, А. Семенченко, О. Соколова, І. Сопілко[11], О. Сосніна, В. Степанова, Ю. Тихомирова, В. Цимбалюка[12], А. Чернобай, М. Швеця. Однак доводиться констатувати, що їхні дослідження носять переважно фрагментарний характер.

Визначення поняття «персональні дані» наводиться в абзаці восьмому статті 2 Закону України «Про захист персональних даних», відповідно до якого персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Але законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які є персональними даними, задля можливості застосування положень Закону до різноманітних ситуацій, зокрема під час обробки персональних даних в інформаційних (автоматизованих) базах і картотеках персональних даних, що можуть виникнути в майбутньому, у зв'язку зі зміною в технологічній, соціальній, економічній та інших сферах суспільного життя.

---

[2] Закон України від 1 червня 2010 р. № 2297-17 «Про захист персональних даних», Закон України від 2 червня 2010 р. №3454-VI «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних», Закон України від 13 січня 2012 р. № 4343-VI «Про внесення змін до розділу II Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» щодо перенесення терміну введення в дію», Указ Президента України від 6 квітня 2011 р. № 390/2011 «Про Положення про Державну службу України з питань захисту персональних даних», постанова Кабінету Міністрів України від 25 травня 2011 р. N 616 «Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення», наказ Міністерства юстиції України від 8 липня 2011 р. № 1824/5 «Про затвердження форм заяв про реєстрацію бази персональних даних та про внесення змін до відомостей Державного реєстру баз персональних даних і порядку їх подання», наказ Міністерства юстиції України від 8 липня 2011 р. № 1823/5 «Про затвердження зразка свідоцтва про державну реєстрацію бази персональних даних», наказ Міністерства юстиції України від 30 грудня 2011 р. № 3659/5 «Про затвердження Типового порядку обробки персональних даних у базах персональних даних», наказ Міністерства юстиції України від 22 червня 2012 р. № 947/5 «Про затвердження Порядку здійснення Державною службою України з питань захисту персональних даних державного контролю за додержанням законодавства про захист персональних даних».

[3] Каретник О. Поняття інформації про фізичну особу (персональні дані) в цивільному праві України. Проблеми цивільного та підприємницького права в Україні. Часопис Київського університету права. 2013. № 2. С. 228.

[4] Брижко В. Організаційно-правові питання захисту персональних даних: дис. ... канд. юрид. наук: спец. 12.00.07. Ірпінь, 2004. 261 с.

[5] Василенко Д., Маслак В. Законодавство провідних країн світу у сфері захисту інформації. Вісник КДУ ім. Михайла Остроградського. 2010. Вип. 2. Ч. 1. С. 128–132.

[6] Гуз А. Історія захисту інформації України та провідних країн світу: навч. посібник. К.: КНТ, 2007. 260 с.

[7] Діхтієвський П. Марченко В. Проблеми використання та захисту персональних даних в умовах загрози інтересам національної безпеки. URL: http://applaw.knu.ua/index.php/arkhiv-nomeriv/1-15-2016

[8] Обуховська Т. Державні механізми забезпечення захисту персональних даних в Україні: дис. ... канд. юрид. наук: спец. 25.00.02. Київ, 2016. 229 с.

[9] Оніщенко О. Захист персональних даних. Юридичний вісник. 2012. № 1 (22). С. 60–64.

[10] Пазюк А. Міжнародно-правовий аналіз інформаційних прав людини в Конституції України. Інтернет- платформа для вчених «Academia.edu». URL: https://www.academia. edu/14102253/

[11] Сопілко І. Механізм захисту персональних даних: проблеми та перспективи. Юридичний вісник. 2013. № 2 (27). С. 66.

[12] Цимбалюк В. Інформаційне право (основи теорії і практики): монографія. К.: «Освіта України», 2010. 388 с.

У контексті збирання таких даних у процесі досудового розслідування варто зауважити, що згідно зі статтею 15 КПК України під час кримінального провадження кожному гарантується невтручання у приватне (особисте та сімейне) життя. Ніхто не може збирати, зберігати, використовувати та поширювати інформацію про приватне життя особи без її згоди, крім випадків, передбачених КПК України. Інформація про приватне життя особи може бути використана не інакше, як для виконання завдань кримінального провадження. Ця норма відповідає статті 32 Конституції України, за якою ніхто не може зазнавати втручання в його особисте та сімейне життя, крім випадків, передбачених Конституцією. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини. Відтак збирання й обробка даних про фізичну особу без її згоди у випадку здійснення цього в межах і для потреб кримінального судочинства мають розглядатись як такі, що здійснюються в інтересах національної безпеки, економічного добробуту та прав людини.

Європейський суд з прав людини неодноразово постановляв, що збирання та зберігання персональних даних поліцією або органами національної безпеки становить втручання у право, гарантоване статтею 8 (1) Європейської конвенції з прав людини. Багато ухвал Європейського суду з прав людини стосуються виправдання такого втручання (наприклад, ЄСПЛ, «Леандер проти Швеції», № 9248/81, 26 березня 1987 р.; ЄСПЛ, «M.M. проти Сполученого Королівства», № 24029/07, 13 листопада 2012 р.; ЄСПЛ, «M.K. проти Франції», № 19522/09, 18 квітня 2013 р.)[13].

Однак сьогодні практично відсутні досконалі методики та надійні техніко-криміналістичні засоби захисту такої інформації. Досить часто матеріали проваджень (їхні електронні версії) зберігаються на особистих комп'ютерах і портативних ноутбуках, котрі не містять адекватних систем захисту від можливої втрати або витоку таких персональних даних. На більшості таких засобів встановлено неліцензійне програмне забезпечення, а під час під'єднання до мережі Інтернет не використовуються досить надійні системи захисту від проникнення в бази даних іззовні. На нашу думку, така ситуація є неприпустимою, оскільки занадто полегшує можливості цілеспрямованого викрадення персональних даних із таких пристроїв, а про належну їхню обробку без ліцензійних програмних продуктів і надійних засобів захисту не може бути й мови.

Іншим аспектом обробки персональних даних у контексті кримінального провадження є проведення дактилоскопіювання осіб, обробка та зберігання цих даних. І хоча можливість пересилання такої інформації в електронному вигляді передбачена (пункт 8.7 Інструкції про порядок формування, ведення та використання оперативно-довідкового й дактилоскопічного обліку в органах внутрішніх справ та органах (установах) кримінально-виконавчої системи України, затвердженої наказом МВС України та Держдепартаментом України з питань виконання покарань N 823/188 від 23.08.2002), все ж домінуючою формою зберігання нині залишається паперова форма. А відтак пересилання таких даних створює реальну загрозу їхньої незаконної обробки, використання та (або) розповсюдження. Створення передумов для масової електронно-цифрової обробки таких даних у межах кримінальних проваджень не лише спростить їхні обмін, обробку та зберігання, але й наблизить нашу державу до європейських інституцій через можливу інтеграцію в такі інформаційні системи на рівні ЄС, як Шенгенська інформаційна система (SIS), Візова інформаційна система (VIS), Євродак (Eurodac).

На стадії судового розгляду захист персональних даних набуває ще більш важливого значення. Одним з аспектів проведення судового розгляду кримінального провадження може бути здійснення заходів забезпечення безпеки (це здійснення правоохоронними органами правових, організаційно-технічних та інших заходів, спрямованих на захист життя, житла, здоров'я та майна цих осіб від протиправних посягань із метою створення необхідних умов для належного здійснення правосуддя (стаття 1 Закону України «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві»). У статті 17 цього Закону зазначено, що у випадках, коли цього потребують інтереси безпеки осіб, узятих під захист, за мотивованою ухвалою суду може проводитися закрите судове засідання. У випадках і в порядку, передбачених Кримінальним процесуальним кодексом України, для забезпечення безпеки учасника кримінального провадження суд за власною ініціативою або за клопотанням учасників кримінального провадження може прийняти рішення про проведення допиту учасника кримінального провадження з використанням відеоконференції за трансляції з іншого приміщення, зокрема, у спосіб, що унеможливлює ідентифікацію особи, яка дає показання. Отже, у законі прямо передбачено високий ступінь захисту персональних даних, однак на практиці відсутня будь-яка регламентація техніко-криміналістичних засобів, які б дали змогу за-

[13] Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2015. С. 157.

безпечити вказане. У таких випадках вважаємо за необхідне закріпити такі засоби захисту персональних даних: використання програмних елементів редагування відео (відповідні затемнені ділянки, що не дають можливості ідентифікувати особу), звичайні засоби гримування, заміна певних елементів одягу. А в ролі засобів, які дають можливість змінити голос, повинні використовуватись лише чітко визначені програмні компоненти (наприклад, можуть використовуватись такі програми, як Clownfish, MorphVoxPro). Принцип роботи таких комп'ютерних програм побудовано на миттєвій редакції звуку, що надходить у мікрофон, його переформатування згідно із встановленими налаштуваннями. Необхідно також узяти до уваги можливість відстеження учасника такої конференції за допомогою визначення IP-адреси (унікальний ідентифікатор кожного комп'ютера в мережі Інтернет, зазвичай записується у вигляді чотирьох чисел через крапки та використовується під час доступу до будь-якого сервера). У цьому випадку видається доцільним встановлювати з'єднання через так-звані проксі-сервери (мережеві програмні комплекси, що дають змогу користувачу звертатися від свого імені до інших мережевих служб, використовуючи посередництво цих проксі-серверів, та бути захищеним від деяких видів мережевих атак, зберігаючи при цьому анонімність).

Останнім аспектом техніко-криміналістичного забезпечення захисту персональних даних виступає належна підготовка місця проведення судового засідання. Особливо ретельно необхідно перевіряти комп'ютерну та іншу техніку в залі судового засідання на предмет під'єднання сторонніх засобів або наявності комп'ютерних програм-шпигунів чи вірусів. До такої перевірки варто додати також і тестування мережевого з'єднання.

Отже, виконання вищезазначених рекомендацій, як видається, дасть змогу суттєво підвищити рівень захисту персональних даних у кримінальному провадженні та сприятиме більш ефективному виконанню завдань кримінального судочинства.

Анотація

У статті аналізується різні аспекти захисту персональних даних у Європейському Союзі та Україні. Проводиться порівняння законодавчого та наукового забезпечення такого захисту. Сфера кримінального судочинства в цьому контексті є особливо важливим аспектом такого захисту через надзвичайну цінність персональних даних, що акумулюються у кримінальних провадженнях. Аналізуються загрози несанкціонованого розповсюдження персональних даних учасників кримінального судочинства у зв'язку зі зберіганням на особистих або портативних комп'ютерних пристроях. Звертається увага на реальну небезпеку можливості несанкціонованого копіювання дактилоскопічної інформації осіб під час пересилання відповідних карт у паперовому форматі. Виокремлюються загрози для зберігання та використання персональних даних безпосередньо на судовому засіданні. Пропонуються відповідні методичні рекомендації та техніко-криміналістичні засоби, які суттєво знижують ризик несанкціонованого розповсюдження персональних даних учасників кримінального судочинства.

Summary

Several aspects of personal data protection in European Union and Ukraine are analyzed in this article. The comparison of normative and scientific securement of such protection is conducting. In this case criminal judiciary system is very important sphere because of extremely high value of personal data that retain inside criminal cases. There was conducted an analysis of several threats concerning illegal dissemination of criminal judiciary participants personal data on private portable laptops. The real danger of fingerprint personal data illegal duplication while its reconsignment is described. Several threats of personal data safekeeping and applying while court hearing are pointed out. A number of methodical recommendations and criminalistic devices are offered to seriously decrease the risk of criminal judiciary participants personal data illegal dissemination.

Використана література:

1. Брижко В. Організаційно-правові питання захисту персональних даних: дис. ... канд. юрид. наук: спец. 12.00.07. Ірпінь, 2004. 261 с.
2. Василенко Д., Маслак В. Законодавство провідних країн світу у сфері захисту інформації. Вісник КДУ ім. Михайла Остроградського. 2010. Вип. 2. Ч. 1. С. 128–132.
3. Гуз А. Історія захисту інформації України та провідних країн світу: навч. посібник. К.: КНТ,2007. 260 с.
4. Діхтієвський П., Марченко В. Проблеми використання та захисту персональних даних в умовах загрози інтересам національної безпеки. URL: http://applaw.knu.ua/index.php/arkhiv-nomeriv/1-15-2016
5. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних. Офіційний вісник України від 14 січня 2011 р., № 1, / № 58. 2010. Ст. 1994. С. 708.
6. Закон України від 1 червня 2010 р. № 2297-17 «Про захист персональних даних». Офіційний вісник України від 9 липня 2010 р. № 49. С. 199.
7. Закон України від 1 січня 2012 р. № 4343-VI «Про внесення змін до розділу II Закону України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» щодо перенесення терміну введення в дію». Офіційний вісник України від 17 лютого 2012р. № 11. С. 50.
8. Закон України від 2 червня 2010 р. №3454-VI «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних». Офіційний вісник України від 4 липня 2011 р. № 48. С. 42.
9. Закон України від 15 березня 1994 р. «Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві». Відомості Верховної Ради України від 15 березня 1994 р. № 11.
10. Каретник О. Поняття інформації про фізичну особу (персональні дані) в цивільному праві України. Проблеми цивільного та підприємницького права в Україні. Часопис Київського університету права. 2013. № 2. С. 228.
11. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Офіційний вісник України від 14 січня 2011 р. № 1, / № 58. 2010. Ст. 1994. С. 701.
12. Конституція України. Офіційний вісник України від 1 жовтня 2010 р. № 72/1. Спеціальний випуск. С. 15.
13. Кримінальний процесуальний кодекс України. Офіційний вісник України від 25 травня 2012 р. № 37. С. 11.
14. Наказ МВС України та Держдепартаменту України з питань виконання покарань N 823/188 від 23.08.2002 «Про введення в дію Інструкції про порядок формування, ведення та використання оперативно-довідкового і дактилоскопічного обліку в органах внутрішніх справ та органах (установах) кримінально-виконавчої системи України».
15. Наказ Міністерства юстиції України від 22 червня 2012 р. № 947/5 «Про затвердження Порядку здійснення Державною службою України з питань захисту персональних даних державного контролю за додержанням законодавства про захист персональних даних».
16. Наказ Міністерства юстиції України від 30 грудня 2011 р. № 3659/5 «Про затвердження Типового порядку обробки персональних даних у базах персональних даних».
17. Наказ Міністерства юстиції України від 8 липня 2011 р. № 1823/5 «Про затвердження зразка свідоцтва про державну реєстрацію бази персональних даних».
18. Наказ Міністерства юстиції України від 8 липня 2011 р. № 1824/5 «Про затвердження форм заяв про реєстрацію бази персональних даних та про внесення змін до відомостей Державного реєстру баз персональних даних і порядку їх подання».
19. Обуховська Т. Державні механізми забезпечення захисту персональних даних в Україні: дис. ... канд. юрид. наук: спец. 25.00.02. Київ, 2016. 229 с.
20. Оніщенко О.В. Захист персональних даних. Юридичний вісник. 2012. № 1 (22). С. 60–64.
21. Пазюк А. Міжнародно-правовий аналіз інформаційних прав люди¬ни в Конституції України. Інтернет- платформа для вчених «Academia.edu». URL: https:.www.academia.edu/14102253/
22. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2015. С. 16–18.
23. Постанова Кабінету Міністрів України від 25 травня 2011 р. N 616 «Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення»/
24. Сопілко І. Механізм захисту персональних даних: проблеми та перспективи. Юридичний вісник. 2013. № 2 (27). С. 66.
25. Указ Президента України від 6 квітня 2011 р. № 390/2011 «Про Положення про Державну службу України з питань захисту персональних даних».
26. Цимбалюк В. Інформаційне право (основи теорії і практики). монографія. К.: «Освіта України», 2010. 388 с.

Yaroslav Bereskyi,
Ph.D., Chair's of Criminal Process and Criminalistics Docent
Ivan Franko National University of Lviv

Valentyn Muradov,
Ph.D., Chair's of Criminal Process and Criminalistics Assistant
Ivan Franko National University of Lviv